**1** A block cipher based pseudo random number generator secure agai key recovery

Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal G. Malkin,

March 2008 **ASI ACCS '08:** Proceedings of the 2008 ACM symposium on Inf computer and communications security

**Publisher:** ACM Request Permissions

Full text available: Pdf (6.48 MB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 13, Downloads (12 Months): 122, Citatic

We study the security of a block cipher-based pseudorandom number g both in the black box world and in the physical world, separately. We fir construction is a secure PRNG in the ideal cipher model. Then, we demc

**2** Optimal communication complexity of generic multicast key distributi

Daniele Micciancio, Saurabh Panjwani

August 2008 **I EEE/ ACM Transactions on Networking (TON)** , Volume 16 I

**Publisher:** IEEE Press

Full text available: Pdf (364.00 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 7, Downloads (12 Months): 123, Citatior

We prove a tight lower bound on the communication complexity of secu distribution protocols in which rekey messages are built using symmetri pseudo-random generators, and secret sharing schemes. Our lower bou

**Keywords**: key distribution, lower bounds, multicast, nested encryptio security

**3** Universally composable and forward-secure RFID authentication an key exchange

Tri Van Le, Mike Burmester, Breno de Medeiros

March 2007 **ASI ACCS '07:** Proceedings of the 2nd ACM symposium on Info computer and communications security

**Publisher:** ACM Request Permissions

Full text available: Pdf (367.90 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 17, Downloads (12 Months): 215, Citatic

Recently, a universally composable framework for RFID authentication p providing availability, anonymity, and authenticity was proposed. In this that framework to address forward-security issues in the presence of ke compromise.We ...

**Keywords**: RFID authentication and key-exchange protocols, anonymit security, universal composability

**4** Low power scalable encryption for wireless systems

James Goodman, Anantha P. Chandrakasan

January 1998 **Wireless Networks** , Volume 4 Issue 1

**Publisher:** Kluwer Academic Publishers

Full text available: Pdf (7.39 MB) Additional Information: full citation, abstract, referer terms

**Bibliometrics**: Downloads (6 Weeks): 10, Downloads (12 Months): 101, Citatic

Secure transmission of multimedia information (e.g., voice, video, data, many wireless network applications. Wireless transmission imposes con in typical wired systems such as low power consumption, tolerance to ..

**5** Hidden credential retrieval from a reusable password

Xavier Boyen

March 2009 **ASI ACCS '09:** Proceedings of the 4th International Symposiun Computer, and Communications Security

**Publisher:** ACM Request Permissions

Full text available: Pdf (752.19 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 11, Downloads (12 Months): 30, Citatior

We revisit the venerable question of access credentials management, w techniques that we, humans with limited memory, must employ to safe access keys and tokens in a connected world. Although many existing s

**Keywords**: online authentication, partially trusted servers, reusable pa stateless roaming credentials

**6** Gaussian random number generators

David B. Thomas, Wayne Luk, Philip H.W. Leong, John D. Villasenor

November 2007 **Computing Surveys (CSUR)** , Volume 39 Issue 4

**Publisher:** ACM Request Permissions

Full text available: Pdf (426.75 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 88, Downloads (12 Months): 865, Citatic

Rapid generation of high quality Gaussian random numbers is a key cap simulations across a wide range of disciplines. Advances in computing h power to conduct simulations with very large numbers of random numb

**Keywords**: Gaussian, Random numbers, normal, simulation

**7** Cryptanalysis of the windows random number generator

Leo Dorrendorf, Zvi Gutterman, Benny Pinkas
October 2007 **CCS '07:** Proceedings of the 14th ACM conference on Comput communications security
**Publisher:** ACM Request Permissions
Full text available: Pdf (238.28 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 16, Downloads (12 Months): 185, Citatic

The pseudo-random number generator (PRNG) used by the Windows op the most commonly used PRNG. The pseudo-randomness of the output is crucial for the security of almost any application running in Windows.

**Keywords:** cryptanalysis, pseudo random number generator (prng), wi system

**8** Protecting bus-based hardware IP by secret sharing
Jarrod A. Roy, Farinaz Koushanfar, Igor L. Markov
June 2008 **DAC '08:** Proceedings of the 45th annual Design Automation Co
**Publisher:** ACM Request Permissions
Full text available: Pdf (604.97 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 9, Downloads (12 Months): 63, Citation

Our work addresses protection of hardware IP at the mask level with th preventing unauthorized manufacturing. The proposed protocol based o activation is applicable to a broad category of electronic systems with a

**Keywords:** computer crime, cryptography, integrated circuits, manufac

**9** Universal nonuniform random vector generator based on acceptance
Gleb Beliakov
July 2005 **Transactions on Modeling and Computer Simulation (TOM/** Issue 3
**Publisher:** ACM Request Permissions
Full text available: Pdf (816.01 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 9, Downloads (12 Months): 52, Citation

The acceptance/rejection approach is widely used in universal nonunifor number generators. Its key part is an accurate approximation of a giver density from above by a hat function. This article uses a piecewise cons ...

**Keywords:** Acceptance/rejection, Lipschitz approximation, nonuniform random number generator

**10** StressTest: an automatic approach to test generation via activity mo
Ilya Wagner, Valeria Bertacco, Todd Austin
June 2005 **DAC '05:** Proceedings of the 42nd annual Design Automation Cc
**Publisher:** ACM Request Permissions
Additional Information: full citation, abstract, referer

Full text available: Pdf (896.33 KB) terms

**Bibliometrics**: Downloads (6 Weeks): 4, Downloads (12 Months): 33, Citation

The challenge of verifying a modern microprocessor design is an overwh Increasingly complex micro-architectures combined with heavy time-to- have forced microprocessor vendors to employ immense verification tea hope ...

**Keywords**: architectural simulation, directed-random simulation, high- simulation

**11** Towards understanding algorithmic factors affecting energy consum complexity, randomness, and preliminary experiments
Ravi Jain, David Molnar, Zulfikar Ramzan
September 2005 **DIALM-POMC '05:** Proceedings of the 2005 joint worksho of mobile computing
**Publisher:** ACM Request Permissions
Full text available: Pdf (234.54 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 2, Downloads (12 Months): 55, Citation

Mobile devices consider energy to be a limiting resource. Over the past research has gone into how one can reduce energy consumption at the network protocol level, operating system level, and compiler level. In al

**Keywords**: energy measurement, randomness cost, switching cost

**12** Simulation in java with SSJ
Pierre L'Ecuyer, Eric Buist
December 2005 **WSC '05:** Proceedings of the 37th conference on Winter sir
**Publisher:** Winter Simulation Conference
Full text available: Pdf (156.90 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 9, Downloads (12 Months): 61, Citation

We describe SSJ, an organized set of software tools offering general-pu stochastic simulation programming in Java. It supports the event view, continuous simulation, and arbitrary mixtures of these. Random numbe

**13** Physical unclonable function and true random number generator: a c scalable implementation
Abhranil Maiti, Raghunandan Nagesh, Anand Reddy, Patrick Schaumont
May 2009 **GLSVLSI '09:** Proceedings of the 19th ACM Great Lakes sympos
**Publisher:** ACM Request Permissions
Full text available: Pdf (558.22 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 26, Downloads (12 Months): 26, Citatior

Physical Unclonable Functions (PUF) and True Random Number Generat two very useful components in secure system design. PUFs can be used unique signatures and volatile secret keys, whereas TRNGs are used for

random ...

**Keywords:** fpga, jitter, macro, puf, ring oscillators (ro), scalable, trng

**14** An SPU reference model for simulation, random test generation and
Yukio Watanabe, Balazs Sallay, Brad Michael, Daniel Brokenshire, Gavin M
Daisuke Hiraoka
January 2006 **ASP-DAC '06:** Proceedings of the 2006 conference on Asia S
design automation
**Publisher:** IEEE Press
Full text available: Pdf (265.87 KB) Additional Information: full citation, abstract, referer
terms

**Bibliometrics**: Downloads (6 Weeks): 2, Downloads (12 Months): 21, Citation

An instruction set level reference model was developed for the developr
synergistic processing unit (SPU), which is one of the key components c
processor [1][2]. This reference model was used for the simulators to d
instruction ...

**15** Automated testing of stochastic systems: a statistically grounded apr
Hana Ševčíková, Alan Borning, David Socha, Wolf-Gideon Bleek
July 2006 **ISSTA '06:** Proceedings of the 2006 international symposium or
and analysis
**Publisher:** ACM Request Permissions
Full text available: Pdf (215.70 KB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 8, Downloads (12 Months): 54, Citation

Automated tests can play a key role in ensuring system quality in softw
However, significant problems arise in automating tests of stochastic alg
Normally, developers write tests that simply check whether the actual r

**Keywords:** hypothesis testing, software engineering, software testing,
algorithms, unit tests

**16** Cryptography using modular software elements
Herbert S. Bright, Richard L. Enison
June 1976 **AFIPS '76:** Proceedings of the June 7-10, 1976, national compu
and exposition
**Publisher:** ACM Request Permissions
Full text available: Pdf (1.40 MB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 1, Downloads (12 Months): 4, Citation C

Protection of information within a computer/communication system can
through reversible cryptographic transformation of the information itself
can be returned to usable form only through use of control information

**17** SEEDEX: a MAC protocol for ad hoc networks
R. Rozovsky, P. R. Kumar
October 2001 **MobiHoc '01:** Proceedings of the 2nd ACM international sym
ad hoc networking & computing

**Publisher:** ACM Request Permissions

Full text available: Pdf (2.30 MB) Additional Information: full citation, abstract, referer terms

**Bibliometrics**: Downloads (6 Weeks): 13, Downloads (12 Months): 77, Citatior

Motivated by the poor experimental scaling reported in a study of the p hoc networks in [15], we propose a new protocol for media access cont networks. Our protocol seeks to avoid collisions without making explicit

**18** D.S.P.P.: a data securily pipe protocol for PC's,large scale systems

Daniel Guinier

November 1988 **SIGSAC Review** , Volume 6 Issue 3

**Publisher:** ACM

Full text available: Pdf (473.26 KB) Additional Information: full citation, abstract, referer terms

**Bibliometrics**: Downloads (6 Weeks): 3, Downloads (12 Months): 11, Citation

D.S.P.P.: Data Security Pipe Protocol is an original asymetric cryptograp dependent public auto-key protocol applied to data security. This protoc designed for secrecy in data files or end-to-end data communications ar problems ...

**19** On the origin of power laws in Internet topologies

Alberto Medina, Ibrahim Matta, John Byers

April 2000 **SIGCOMM Computer Communication Review** , Volume 30 Issue

**Publisher:** ACM

Full text available: Pdf (1.22 MB) Additional Information: full citation, abstract, referer

**Bibliometrics**: Downloads (6 Weeks): 7, Downloads (12 Months): 86, Citation

Recent empirical studies [6] have shown that Internet topologies exhibi the form $y = x^{a}$ for the following relationships: (P1) outdegree of node router) versus rank; (P2) number of nodes versus ...

**20** Pseudo-random generators for all hardnesses

Christopher Umans

May 2002 **STOC '02:** Proceedings of the thiry-fourth annual ACM symposiu computing

**Publisher:** ACM Request Permissions

Full text available: Pdf (234.48 KB) Additional Information: full citation, abstract, referer terms

**Bibliometrics**: Downloads (6 Weeks): 3, Downloads (12 Months): 21, Citation

(MATH) We construct the first pseudo-random generators with logarithr that convert $s$ bits of hardness into $s^{\Omega(1)}$ bits of 2-sided pseudo-randomr This improves [8] and gives a direct proof ...